Scientific Research Publishing

Circuits and Systems, 2016, 7, 3504-3521
http://www.scirp.org/journal/cs
ISSN Online: 2153-1293
ISSN Print: 2153-1285

CAND-IDS: A Novel Context Aware Intrusion Detection System in Cooperative Wireless Sensor Networks by Nodal Node Deployment

Rathinam Gopal[1], Velusamy Parthasarathy[2]

[1]Department of Computer Science and Engineering, Chettinad College of Engineering & Technology, Puliyur, Karur, Tamilnadu, India
[2]Department of Computer Science and Engineering, Veltech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Chennai, India
Email: rgopalkarur@gmail.com, sarathy.vp@gmail.com

How to cite this paper: Gopal, R. and Parthasarathy, V. (2016) CAND-IDS: A Novel Context Aware Intrusion Detection System in Cooperative Wireless Sensor Networks by Nodal Node Deployment. *Circuits and Systems*, **7**, 3504-3521.
http://dx.doi.org/10.4236/cs.2016.711298

Received: April 24, 2016
Accepted: May 15, 2016
Published: September 7, 2016

Copyright © 2016 by authors and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

Cooperative wireless sensor networks have drastically grown due to node co-operative in unaltered environment. Various real time applications are developed and deployed under cooperative network, which controls and coordinates the flow to and from the nodes to the base station. Though nodes are interlinked to give expected state behavior, it is vital to monitor the malicious activities in the network. There is a high end probability to compromise the node behavior that leads to catastrophes. To overcome this issue a Novel Context Aware-IDS approach named Context Aware Nodal Deployment-IDS (CAND-IDS) is framed. During data transmission based on node properties and behavior CAND-IDS detects and eliminates the malicious nodes in the explored path. Also during network deployment and enhancement, node has to follow Context Aware Cooperative Routing Protocol (CCRP), to ensure the reliability of the network. CAND-IDS are programmed and simulated using Network Simulator software and the performance is verified and evaluated. The simulation result shows significant improvements in the throughput, energy consumption and delay made when compared with the existing system.

Keywords

Cooperative Network, Intrusion Detection System, Context Aware Routing Protocol, Network Simulator

1. Introduction

In the past ten years, wireless sensor network is getting more important due to various applications which make use of emerging technology. One of the main advantages of

wireless sensor networks is that the fundamental devices used are cheap, intelligent which function in various network configurations. Wireless sensor networks can send and receive different types of data with various applications [1]. The earliest applications of sensor networks are mainly used in military, surveillance systems and hospitals [3]. In those days the sensor devices are connected through wires. Then radio communications are used for connecting sensor devices and it leads to creating more novel applications [2]. Nowadays telecommunication market needs heterogeneous communication devices and technologies [4]-[7]. From wired network to wireless, cellular networks need LTE, 3G and 4G technologies for providing internet access. Since, it is essential to have cooperation amongst these technologies to provide better future heterogeneous communication. In [8], the author focuses on the context-aware data transmission using cooperative satellite networks, because delivering the data should reach the user without fail. In [9] the detection of malicious nodes is done using the algebraic watch dog by watching the receiver side transmission. In [10] the energy consumption is decreased and the intruders among the military are detected using a human body sensor.

Cooperation among different devices in a multi-communication network is always a major issue. To provide the effective access between the hybrid networks a single strand protocol is required, which accepts the mobility based access and delivers the useful information to the end users. Cooperative network is an efficient mode to explore the quality in ad hoc, cellular, vehicular and wireless sensor networks. The prime focus is to distribute or share the load between the nodes and thus by extending the life time. Cooperative network is essential because of distinct technologies utilized by various networks; there may be a significant impact on the users perceived service quality and resource utilization. The devices participating in the cooperative network should co-operate each other in terms of communication. Some of the generic features are to be corrected in MAC layer that will enable new protocol that supports in a cooperative network. The control elements in the cooperative network should not have keen account about the communication. It gives the platform to find the useful information between the global accesses. Major issues like routing updating, relaying and network coding are cumbersome. In case of heavy traffic the cooperative process functionally reduces its performance due to various reasons. Apart from data transmission, each node work is loaded to be a monitor node for other nodes in the network, secured way of information exchange between the nodes or between the networks, exploring alternate path in the network by local decision if malicious node identified. Detection is a common process which calls unconditionally at each node. If any detection means, information exchange will not happen, and leads to block the node with the help of the base station. The node which is called malicious by cooperation coefficient [11] with respect to the other nodes is done by consensus approach.

In the proposed approach, a nodal node is selected and whenever a node wants to transmit then a path is generated which comprises the nodal node. The nodal node has the control over the transmission. Nodes other than the nodes in the path are considered as malicious nodes and those nodes are eliminated from the path and the network.

2. Background Study

In the cooperative network the malicious activity can disturb the network performance [12]. To detect and eliminate the malicious activity the honest nodes are identified and transmit. Then block and eliminate the malicious nodes from the network. To do this, a reputed system needs to provide a trust calculation mechanism during the device access [13]. CONFIDENT reputation technique was proposed to observe the nodes trustiness and report to BS [14].

Yiqing Zhou *et al.* [15] investigated both transmitter and receiver uses multiple antennas to fight against wireless fading and link throughput. They proved through simulation that the power ration depends on the number of antennas, the number of pilots and the data symbols in the packet. In cases like sensor nodes and handheld devices, they have very less physical size and power which make multiple antennas implementation more difficult.

Laneman *et al.* [16] reported that, cooperation among the users in the network is essential to obtain spatial diversity by making the availability of the user terminals where it can be used to share their antennas from the collection of antennas. Cooperative network is mainly used for resource allocation and resource sharing [17]. Performance analysis of optimizing the resource cooperation [18] [19] is discussed for choosing best cooperative resources for improving the performance. A cooperative medium access control (MAC) and designing a routing mechanism is presented in [20] [21] in which the throughput and reliability of the wireless transmission increases based on the user cooperation.

Wireless channels physical characteristics are exploited implementing the security at physical layer. This technique in turn prevents intruders from intercepting the transmission between the sender and the receiver. Wyner *et al.* [22] and Leung Yan Cheong *et al.* [23] investigated a technique called secrecy capacity in which the channel capacity between the source and destination and that the channel capacity between source and intruder. If the value of the secrecy capacity is positive then the intruder will fail and if the value is positive then the intruder will success in intercept made. The security issues and challenges are discussed in [24]-[26] and provide a coopMAC for MAC layer based secured communication in the networks.

Wireless sensor network has certain limitations such as it should operate the nodes in specific energy level, there should be a possibility scarcity of the node, and no equal-distance approach maintain between the nodes though they were connected. Traffic between the nodes during communication is a major issue. Load on nodes due to overlap reduces the energy level high. To overcome these anomalies, certain measures are identified and implemented in proposed Context Aware Cooperative Routing Protocol.

3. Problem Statement

In this paper detecting and eliminating malicious nodes using the proposed approach named CAND-IDS method. Where detecting the malicious node by monitoring all the sensor-nodes through nodal nodes in the network. The nodal node is deployed in all

the layers where the number of nodal node is 1% of the total number of nodes deployed in the layer. Nodal nodes are monitoring and verifying the behavior and properties of the sensor-nodes in the explored path before data transmission. Verification is applied during and after data transmission, hence CAND-IDS can detect and provide prevention for malicious activities. In the earlier research work, the author attempt to analyze the route [11] during data transmission for detecting intrusion. There are chances malicious nodes can occur after route discoveries then it disturb the network during data transmission. Also, malicious activities can be created In and Out of the route. The existing approach verifies only the nodes in the route. But our proposed CAND-IDS verify the nodes in the layers. Hence our approach is efficient in monitoring and eliminating malicious nodes is more accurate than the existing approach.

4. Context Aware Cooperative Routing Protocol

CCRP is flexible for node deployment, it is reliable with system behavior, it is scalable in terms of number of nodes and the size of the network increases and it is available throughout the communication. CCRP extends its functionality for various types of application under various domains. Since, it is cooperative network, nodes under CCRP cooperate with each other, aware the behavior of other nodes and they can easily identify the misbehavior node under various situations.

4.1. Network Model

Consider a network $G = (V, E)$, V is the set of all sensor nodes and E is the communication pointer between the sensors. Though it is connected graph it doesn't mean that all sensor nodes interconnected with each other and it is cooperative. The path is the ways which nodes are identified between sources and sink node and it is open-path based on the nearest neighbor node. The basic assumption is the explored path doesn't contain any cycle. The explored path must have one or more nodal nodes which act as a bridge between the sensor nodes in the path. Nodal node which in turn called as sensor node will keep track information about the set of nodes attached to this nodal node. The node is able to transmit data to any node in the network, nodes are deployed in random manner and all nodes are static in nature. Node to be added to the network based on the following conditions.

1) Node energy is greater than or equal to the commanded value.

2) The node should have a specific amount t of internal storage which is used to support during data transmission in case of any failure.

4.2. Network Communication Model

In this paper, it is assumed that the topology of the network is mesh, but the connections between the nodes are applicable when it requires. The network is differentiating in specific levels; each level has certain nodes [shown in **Figure 1**]. Out of these nodes, a node which has high energy and centric to access between the layer nodes is called as nodal node.

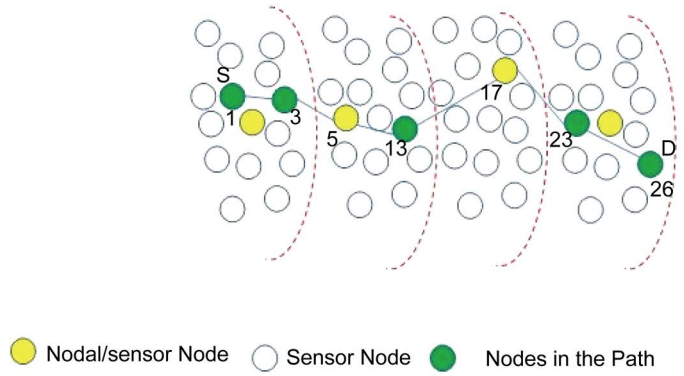

Figure 1. Network model.

Nodal Node in each layer is selected by:

Let $N = \{N_1, N_2, \cdots, N_m\}$

$L_1 = \{N_1, N_2, \cdots, N_i\}$

$L_2 = \{N_1, N_2, \cdots, N_j\}$

…

$L_n = \{N_1, N_2, \cdots, N_k\}$

where $(L_1 \cup L_2 \cup L_3, \cdots, \cup L_n) = N$.

L_1 is the highest energy gain nodes

L_n = centric node can access easily by all other nodes in the layer

$S_n = (G_N \cap L_n)$

NN_1 <- S_N and these above criteria is considered for all the other layers.

A set of associated nodes in the path identified for data transmission is monitored and controlled by this nodal node. It has a provision to initiate data transmission or to skip some of the node associated with it from data transmission. The only restriction is this nodal node access is limited, to ensure safety access throughout the path.

The path considered for data transmission is {1, 3, 5, 13, 17, 23, 26} where 1 and 26 are the source and destination nodes available in the open-path depicted in Figure 1. Nodes 5 and 17 are the nodal nodes, where node 5 controls and monitors set of nodes {1, 3, and 13} whereas node 17 controls and monitor set of nodes {13, 23, and 26}. These nodal nodes keep track of information of all nodes associated with it. The information includes location, energy level and node identity. If any node trying to misbehave or compromise during data transmission by false identity these nodal nodes identify it and send the information to the base station about the malicious node. The base station will take further action by eliminating the malicious node while establishing networks in the next round.

As per the protocol each node has internal storage to keep a replica of data packet if the sensor node is considered as nodal. Due to the different rounds nodal node will change according to energy level. Throughout the data transmission till sink node receives data, the nodal node participated in the path will keep redundancy of the data packet. This process is also called as **"efficient check point"** technique. After successful

data transmission redundant data packets from nodal nodes is cleared along with the path. In case of contingency, the nodal node which has information about the data transmission where the data packet get lost. Hence, it initiates the transmission from the corresponding nodal node instead of transmitting from the source node. The general assumption here is nodal node has to wait for commendable timing which includes minimum delay between the nodes transmitted to a next nodal node. Once the data packet reached to next nodal node the previous nodal node shall reset the data packets stored. It makes the efficiency in terms of memory maintenance and less time.

5. Context Aware Nodal Deployment-Intrusion Detection System (CAND-IDS)

Each node activity is monitored by nodal nodes in the layer. Here the algorithm identifies malicious nodes where 1) the node is a non-nodal node; if the node is not a part of the path in a data transmission and it is accessing the non-nodal sensor node in a path with different identity may or may not represent the other non-nodal nodes in the path. In this case, based on node information the nodal node easily identifies the nodes which try to compromise the node in the path and sends the information to the base station. If the node is considered as a compromised node in the path, in this case nodal node dismantle the path considered for data transmission and provides the information about the compromised node to the base station. Base station initiates the data transmission between the source and destination with different path by eliminating the compromised node permanently. 2) The node is a nodal node. If the nodal node is actively as a compromised node, then it reacts to explore the new path or it monitors and control beyond the allotted nodes in the path. In this case, data transmission is called OFF by the base station to establish data transmission between the source and destination with new nodal nodes. Say node N_y is a nodal node, $N_y \in$ Path-P. Where $P = \{N_1, N_2, N_3, \cdots, N_y, \cdots, N_n\}$. N_y is assigned to monitor $\{N_{y-2}, N_{y-1}, N_{y+1}\}$. If N_y monitors N_{y+2} which $\notin N_y$ set. Then N_y is declared as compromised node.

Phase 1:

CCRP ( )

1. {
2. $G = (V, E)$ where V represents the collection of nodes and E represents the connection among the nodes.
3. $V = N = \{N_1, N_2, N_3, \cdots, N_n\}$ where $\forall N_i \in N$
4. $L = \{L_1, L_2, \cdots, L_L\}$ where $\forall L_i \in L$, the set of levels in the network
5. for $I = 1$ to n
6. for $J = 1$ to L
7. for $K = 1$ to n/L
8. $N_i \xrightarrow{\text{deployed}} L_i$ //n/L number of nodes are placed in layer L_i
9. end K
10. end J
11. end I

12. // input : path P
13. // output: Nodal-nodes $\{N_{n1}, N_{n2}, \cdots, N_{mn}\}$
14. // Prerequisite : path $P \in G = 1$
15. // Initial condition: Network with layers separated
16. // exit criteria: graph G $\notin$ connected graph or all nodal nodes are identified in layer $L_1, L_2, \cdots, L_n$
17. Check_Point (path P)
18. CAND_IDS (path P)
19. }

Phase 2:

Check_Point (path P)

1. {
2. $P = \{N_1, N_2, \cdots, N_{y-1}, N_y, N_{y+1}, \cdots, N_n\} \in G$
3. Identify layer "L_i"
4. do {
5. j = node(i)
6. identify high energy level of all the nodes in the level i
7. N_j = Nodal-node for energy level(i)
8. i++
9. } while(i! = null);
10. $N_j \in G$ in level $L_1, L_2, \cdots, L_n$
11. If (path "P" exists) then
12. net_path = P and N_{nodal}
13. N_{nodal} = set_assigned(P)
14. end if
15. }

Phase 3:

CAND_IDS (path P)

{

//Input: valid path P

//Output: IDS_node/Null

//Prerequisite: path P is validated by check_point ( )

//Initial Condition: Nodal nodes in the path P with valid check

//Exit Criteria:
$0 \Rightarrow$ if network failur
$-1 \Rightarrow$ if nodal bcomes compromised
$-2 \Rightarrow$ if sensor node compromises nodal non-nodal in the path
$-3 \Rightarrow$ if nodal preemptively calls BS to stop

1. enum e1{eEnable, eDisable, eError}
2. -- non-nodal sensor node with non-nodal path node
3. if(!path(sensor-node)) then
4. if (sensor-node.logic == eEnable) then

```
5.                  if (sensor-node is acquiring P(sensor-node). info in path P) then
6.                  declare sensor-node.logic = eError
7.                  sensor-node.alertflag = true
8.                  send(sensor-node.location, sensor-node.info, −2)  ⇒ BS
9.                  stop data-transmission
10.                 restart CCRP ( )
11.             else
12.                sensor-node.logic == eEnable
13.         end if
14. end if
15. -non-nodal-node acts as a compromised node
16.   if(path(sensor-node)) then
17.             if (sensor-node.logic == eEnable) then
18.                 if (sensor-node is acquiring G(sensor-node)) then
19.                 declare sensor-node.logic = eError
20.                 sensor-node.alertflag = true
21.                 send(sensor-node.location, sensor-node.info, −2)  ⇒ BS
22.                 stop data-transmission
23.                 restart CCRP ( )
24.             else
25.                sensor-node.logic == eEnable
26.           end if
27. end if
28. - nodal - node act as a compromised node
29.   if(path(nodal-node)) then
30.             if (nodal-node.logic == eEnable) then
31.                 nodal-node (monitor-node  N ∉ N_Nodal )
32.                 declare nodal-node.logic = eError
33.                 nodal-node.alertflag = true
34.                 send(nodal-node.location, nodal-node.info, −1)  ⇒ BS
35.                 stop data-transmission
36.                 restart CCRP ( )
37.             else
38.                nodal-node.logic == eEnable
39.           end if
10. end if
41. - preemptive terminate of data transmission
42. send(nodel-node.path, −3)  ⇒ BS
43. clear path (P)
44. disable all flags
45. end
46. }
```

Algorithm for CCRP

Step 1: Initialize the network G with nodes deployment and the connection between them.

Step 2: Select the node N and the layer L in which it will be placed. *i.e.* n/L nodes will be placed in a layer L_i.

Step 3: List out the number of layer L_1, L_2, L_3, ⋯, L_n and the nodes present in it.

Step 4: Exit if all the nodal nodes (N_{n1}, N_{n2}, ⋯, N_{mn}) are identified in all the layers separated.

Algorithm for Check_point

Step 1: Find out all the nodes that are in the network G.

Step 2: For each layer Li, do the following:

1) Select the nodes that present in concerned layer Li.

2) Calculate the energy of all the nodes in that layer.

3) The node with the highest energy level will be elected as the nodal node for that layer.

Step 3: The step 2 has to be repeated for the other layers present in the network and the nodal node has to be elected as above.

Step 4: Select the path between the source and the destination with the nodal node in the selected path. Nodal node will have the details about the path and then it controls the transmission in it.

Algorithm for CAND_IDS

Step 1: Valid path given by the Check_Point will be the input.

Step 2: If any node not in the path tries to forward data to the nodes in the path then the nodal node will consider it as malicious and information about location of that node will be forwarded to the Base station. Base Station will eliminate this node from the network and in the future communications.

Step 3: If the node present in the path act as malicious node then the nodal node will stop the data transmission of that node and inform the base station.

Step 4: If the nodal node acts as a malicious node and if it tries to communicate with a node which is not a nodal node then the data transmission will be stopped.

CCRP algorithm initializes the network by node, node deployment, assigning nodal nodes based on higher energy and centric to the respective levels of the network. Based on the number of nodes in each level nodal node is identified by 1 to 2. If a node N_i needs to transmit data to node N_j then a path P is established inclusive of nodal nodes. Nodal nodes keep the information of data packets handled throughout the transmission. After successful delivery of data packet to next nodal node or to a destination node, the current nodal node shall clear the data information. In case of contingency, the latest nodal node is considered to initiate the data transmission from that point to destination node as per path information. If a sensor-node which is not considered in the path P but it is connected to graph G is considered as a compromising node tries to communicate with other sensor node in path P. Through this algorithm particular node is treated as a malicious node and information regarding the node is transferred to the

base station (BS). BS will consider the issue by location information of the malicious node and eliminates the node from the network present and in the future rounds. If a sensor-node which is considered as a non-nodal node in path P, is ensured as malicious node and trying to communicate with other nodes which are not really communicable. In this case, nodal node identifies the malicious node and stops the data transmission with immediate effect and the same can be informed to BS and algorithm will initiate by eliminating malicious node. If a nodal node in the path P is identified as a malicious node and trying to communicate with the nodes in which nodes are not associated with the nodal set. In this case, BS calls OFF the data transmission by eliminating nodal node which misbehaves from the network and recalls the algorithm.

Theorem-1:

Let U be set of nodes which is finite and S be the set of nodes in path P and T' be the complement of S and then $\exists(P) \Rightarrow S \bigcap T' = \varnothing$.

6. Simulation Settings

The check point algorithm is coded in TCL language and simulated in Network Simulator-2. The parameters assigned for simulating the proposed CAND-IDS is given in Table 1.

CCRP is derived from AODV protocol and many rounds of simulation are applied to verify the performance. Various rounds are verified with different number of nodes deployed in the network and it leads to verify the path with different number of nodes based data transmission effectiveness. In the initial round the node number is less compared with the other rounds and the measured performance value is also less. The performance is calculated in terms of number of malicious activities detected, throughput, energy and time taken for transmission with and without CAND-IDS inclusion. The obtained results are shown in Figures 2-8.

Table 1. Simulation parameters used.

Parameter	Values Assumed
Examined Protocol	AODV, CCRP
Number of Nodes	100, 200, 300, 400, 500
Simulation Area Dimension	1200 × 1200 sq m
Simulation Time	50 Sec
Radio range	250 m
Traffic Type	CBR, 5 pkts/s
Packet Size	256 to 512
Traffic Connections	TCP/UDP
Node Speed	10 m/s
Type of Attack	Generic

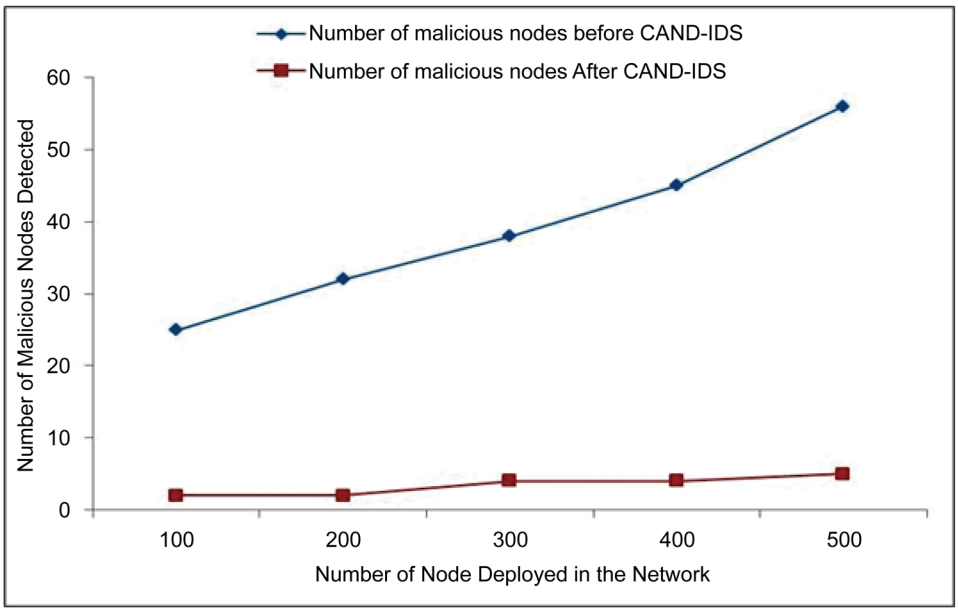

Figure 2. Malicious activity detection before and after CAND-IDS.

Figure 2 shows the participation of nodal node, path information along the nodes in the path which is considered for data transmission is clearly visible. Hence the malicious node detection is affirmative in the path. Else some of the other nodes are to allot for identifying malicious node in the network. This is tedious work and extra load to the nodes in the path or on the network. Comparatively, malicious node occurrence is less due to a protocol which is applied in the node deployment. In each round of the simulation, the numbers of nodes are exercised in increasing order; say in case of 100 nodes, the number of malicious nodes detected is around 3 to 4. For the most possible extent deployment protocol, which is active in nodal introduction, will take care of certain security measures for node identity. In the next round of node deployment, say 400 nodes, the number of malicious nodes detected is 7 to 8 which is really affirmative.

Figure 3 shows the phenomenon that is to identify the nodal node in each layer gives the complete bridge between the layers and to identify the path. Entire nodes participating in the path are controlled and monitored by nodal nodes. These are the sensor node, which keep the replica of the data packet, and monitors the set of nodes associated with it. Number of nodal nodes in the path depend upon the number of sensor nodes becomes active in the route. If number of nodes increases or path length holds the highest number of sensor nodes, nodal node selection also increases. Say network has 100 nodes in the initial round; let us assume 4 layers are capable of holding the sensor node information. So that's 4 to 5 nodal nodes were created in a dynamic fashion to keep track an eye of all sensor nodes in the respective layer. In case of path generation this nodal layer which is identified is become active to enhance the data transmission. In increasing case of nodes in the network layer is reformed and nodal node selection is reframed based on high energy and centric to the layer. Numbers of nodal nodes deployed in the network are shown.

Figure 4 shows the load of the node in the network is equally distributed, in the case of monitoring nodes; nodal nodes as well as nodes are in data transmission. In each round high energy nodes are selected as nodal nodes to monitor other sensor nodes. It will be round robin in nature. Let us say for 200 nodes of network, 8 nodal nodes were identified to cover all 8 levels. Whereas, energy wise 99% of nodes remains idle, in the case of data transmission, path nodes wake up and continue in operation and gone to sleep mode and initiate wait state again. If number of nodes in the network increases, monitor node energy only used to keep an eye over the other sensor nodes in the layer. This also dynamic selection, so no single node will be always acted as a monitor node or nodal node. Energy efficiency wise the algorithm is working on expected way, by earlier

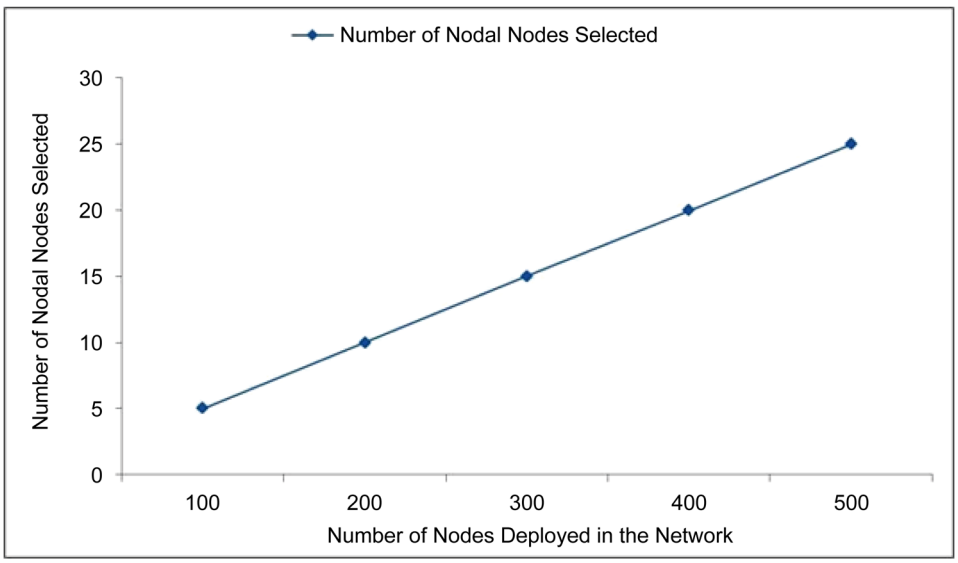

Figure 3. Number of nodal nodes selected.

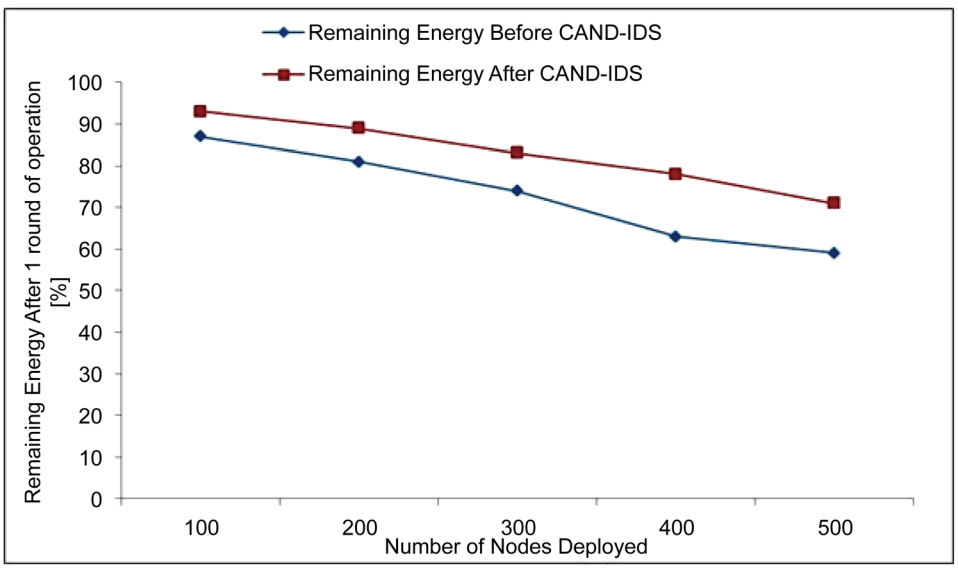

Figure 4. Remaining energy comparison before and after CAND-IDS.

approach the energy efficiency is a cumbersome when number of nodes are participated in a huge manner. The remaining energy after one round for various numbers of nodes in the simulation is shown.

Figure 5 shows the throughput obtained by CAND-IDS proposed algorithm simulated with different number of nodes in a different iteration. Say if 100 numbers of nodes are considered, throughput, the amount of data is transferred or processed between the nodes. 1.5 Kbps data is transferred in the amount of time. The same is extended to 3 Kbps when the numbers of nodes are exercised for 500 nodes.

Figure 6 shows the time taken for one round of operation in CAND-IDS algorithm. Each process in the node is determined dynamically and all the nodes in the path will

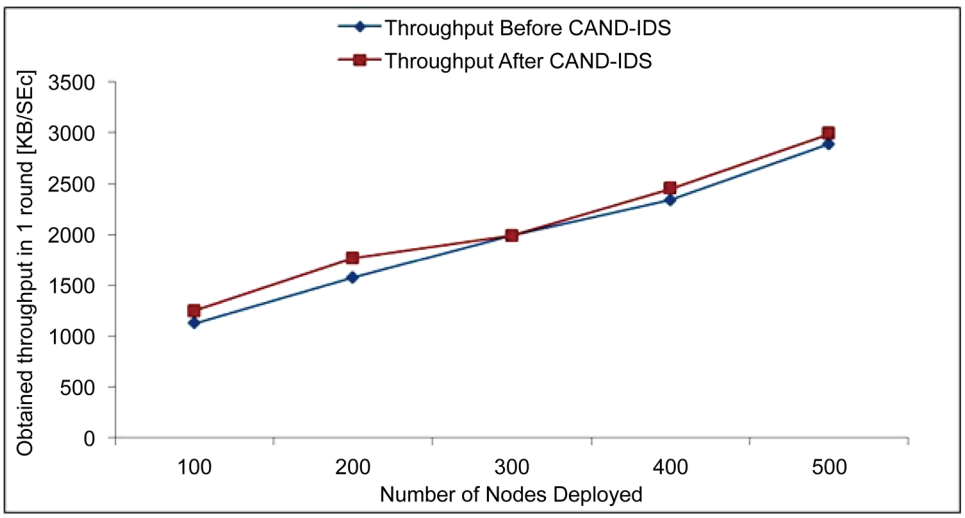

Figure 5. Throughput comparison before and after CAND-IDS.

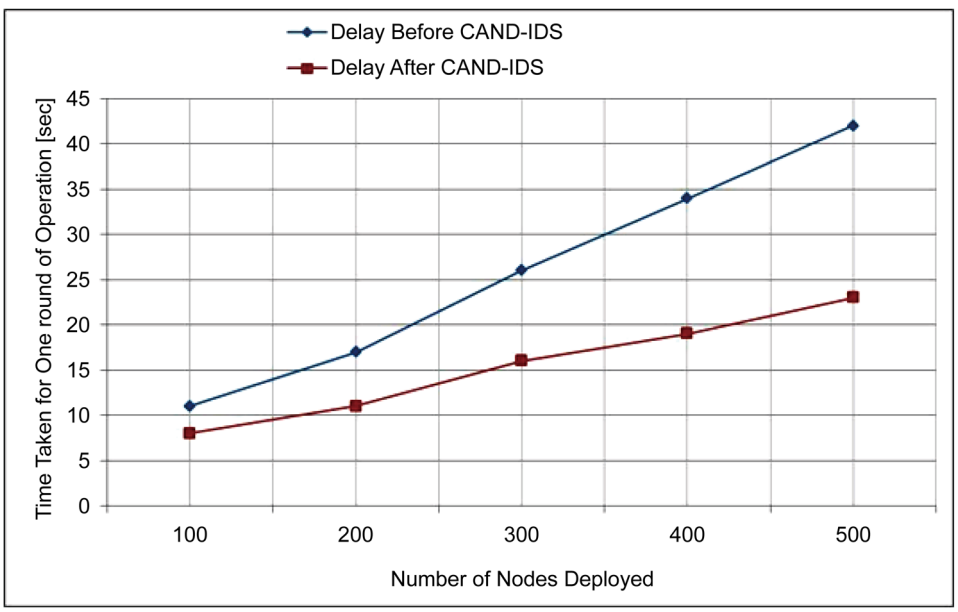

Figure 6. Time taken for one round of operation before and after CAND-IDS.

be active to complete the data transmission. There is a minimum delay which has been noticed in the proposed approach, whereas earlier approach leads to stall for minimum or fixed delay in each case. Say for 100 nodes, time taken for a single round of operation, it requires 6 to 7 seconds. 18 to 19 seconds is recorded in case of 500 nodes deployed in a network.

In Figure 7, for simulation strategy, all kinds of threats were exercised; each threat is executed for 100 to 500 nodes of step count 100. Considering the Sybil attack, for 100 to 200 nodes no Sybil were deducted, this is due to protocol restriction during node deployment, for the 300 node algorithm is tracked 3 nodes as malicious and for 400 to 500 nodes in the network, there is a possibility of 4 Sybil nodes as an outcome. Nodal nodes will identify this Sybil when false identity is accessed, any of the nodes by this algorithm and immediate action will be taken place. Sinkhole attack is exercised for 100 to 500 nodes for a step count of 100. The algorithm allows identifying 1 attack for 200 nodes, which is passive and not transmitted data packet to the appropriate node. When node number is exercised for 2400 to 500, number of sink hole triggered is 2 to 3. Hence the algorithm satisfactorily found the sink hole in all norms. Similarly for DoS attack nodes, the algorithm will be working in fine mode, to identify the intruder in large means; mostly all near to the number of DoS attacks were identified.

Assume for 100 nodes 5 DoS attack node is exercised, the algorithm will refine all the 5 attack nodes and removal the same before data transmission. In further iterations, nodes were exercised for 500 and 9 intruder is considered as DoS, all the DoS attack nodes were identified and removed for layer and path interaction. Similarly for DDoS attacks the nodal nodes will identify the intruder; here this attack will be common to become compromised node in a network. Though the entry protocol defines set of rules for node, this DDoS will be generic to the environment; identification includes all the DDoS for the extent and eliminates it and network is reframed with all the remaining

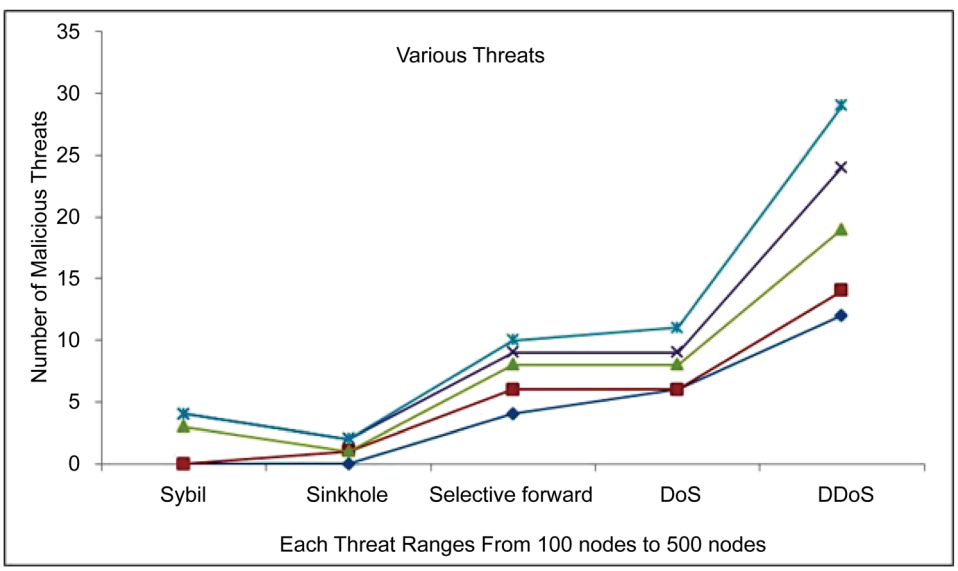

Figure 7. Various threats simulated in various rounds.

nodes. Say for 300 nodes it detect 15 nodes out of 17 intruder nodes. Same for 500 node environment out of 28 nodes 27 intruder nodes were detected. Comparatively the algorithm suits to identify all the above said threat through nodal node analysis.

7. Performance Evaluation

The performance of the proposed approach is evaluated by comparing the performance metrics, delay, throughput and detection rate is calculated and compared with the existing approach LBIDS, DAD [24] [27] and shown in Figures 8-10. In this paper LBIDS and CAND-IDS are simulated in network simulator for various numbers of nodes deployed in the network such as 100, 200, 300, 400 and 500. Figure 8 illustrates the comparison of

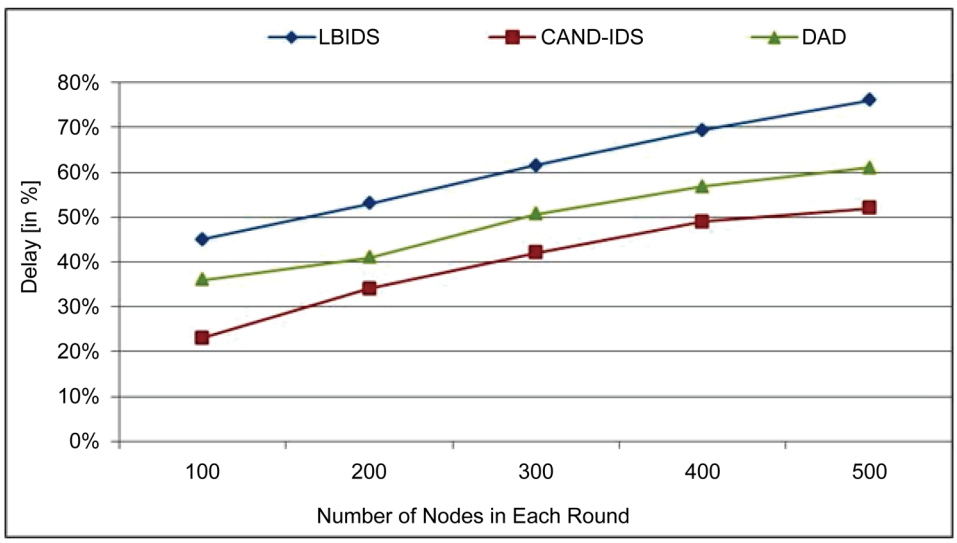

Figure 8. Delay comparison between LBIDS vs. CAND-IDS vs. DAD.

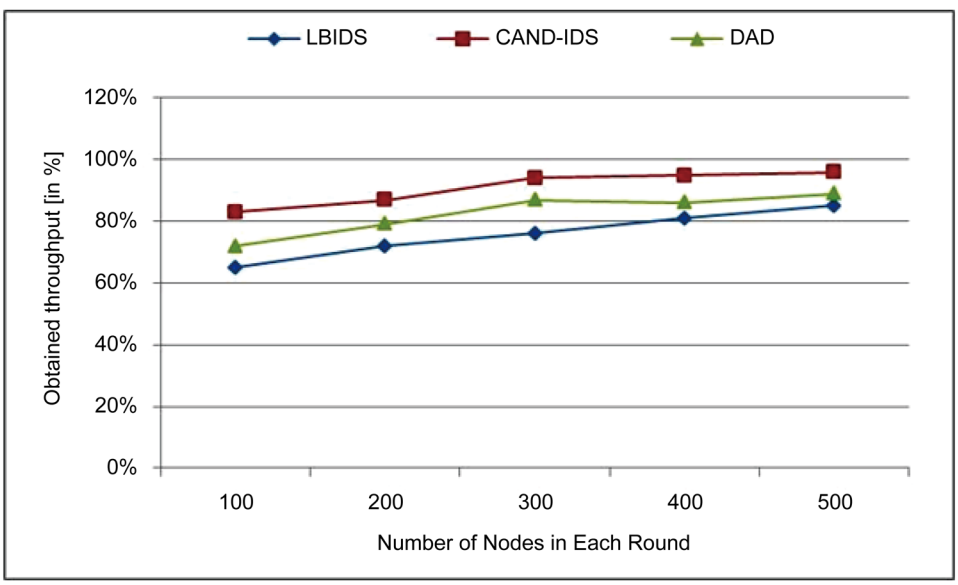

Figure 9. Throughput comparison between LBIDS vs. CAND-IDS vs. DAD.

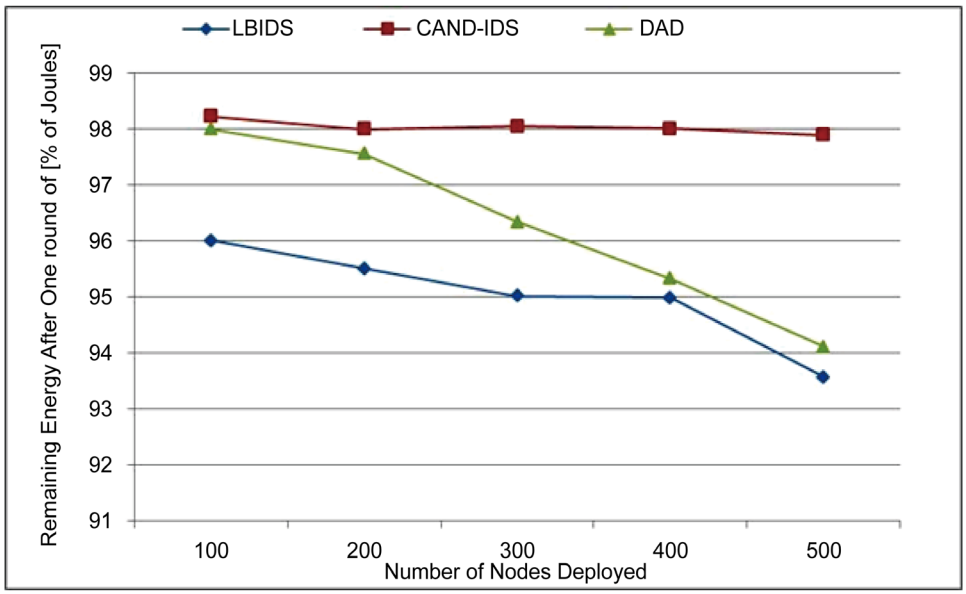

Figure 10. Remaining energy comparison between LBIDS vs. CAND-IDS vs. DAD.

delay taken by the LBIDS and CAND-IDS methods in terms of number of nodes. From Figure 8, it's clear that the delay taken by the proposed CAND-IDS is less than the existing approaches LBIDS and DAD. Similarly, CAND-IDS obtained higher throughput than the LBIDS and DAD. In terms of energy CAND-IDS consumes less energy than the LBIDS and DAD in all the rounds of operation and it's shown in Figure 10 clearly.

8. Conclusion

This paper describes the way of detecting and preventing malicious activity by monitoring approach. The proposed approach doesn't affect the performance of the normal network functionality such as throughput, delay and energy consumption. The proposed approach has lots of benefits which make the cooperative network functions well than other networks without getting affected by any malicious threats. CAND-IDS provide a precise guideline for making efficient protocol for improving the QoS. The performed simulations are motivated to assess the efficacy of the proposed approach in terms of malicious detection without affecting the network behavior. The simulation is designed to obtain the entire performance variable by deploying various numbers of nodes in various rounds. From the simulation results CAND-IDS proved itself and it is an efficient method and its performance is better than the existing approach LBIDS in terms of energy consumption, throughput and delay taken. In future CAND-IDS can be extended by including data security using efficient cryptography method. Data security has not been considered in CAN_IDS and in a communication; security of the data is as important as the communication. A natural continuation of this work is to enrich the set of simulations to test variations in relevant factors or importance that were not considered in this work and their statistical analysis trying to discover relations among the factors which are identified in the experiments so far.

References

[1] Akyildiz, I.F. and Kasimoglu, I. (2004) Wireless Sensor and Actor Networks: Research Challenges. *Ad-Hoc Networks*, **2**, 351-367. http://dx.doi.org/10.1016/j.adhoc.2004.04.003

[2] Whitman, E.C. (2005) SOSUS: The "Secret Weapon" of Undersea Surveillance. *Undersea Warfare*, **7**.

[3] Kuorilehto, M., Hannikainen, M. and Hamalainen, T.D. (2005) A Survey of Application Distribution in Wireless Sensor Networks. *EURASIP Journal on Wireless Communication and Networking*, **2005**, 774-788. http://dx.doi.org/10.1155/WCN.2005.774

[4] Kawamoto, Y., Nishiyama, H., Fadlullah, Z.M. and Kato, N. (2013) Effective Data Collection via Satellite-Routed Sensor System (SRSS) to Realize Global-Scaled Internet of Things. *IEEE Sensors Journal*, **13**, 3645-3654. http://dx.doi.org/10.1109/JSEN.2013.2262676

[5] Sakano, T., Fadlullah, Z.M., Ngo, T., Nishiyama, H., Nakazawa, M., Adachi, F., Kato, N., Takahara, A., Kumagai, T., Kasahara, H. and Kurihara, S. (2013) Disaster-Resilient Networking: A New Vision Based on Movable and Deployable Resource Units. *IEEE Network Magazine*, **27**, 40-46. http://dx.doi.org/10.1109/MNET.2013.6574664

[6] Fadlullah, Z.M., Nishiyama, H., Kato, N. and Fouda, M.M. (2013) Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks. *IEEE Network Magazine*, **27**, 51-56. http://dx.doi.org/10.1109/MNET.2013.6523809

[7] Kawamoto, Y., Nishiyama, H., Kato, N. and Kadowaki, N. (2013) A Traffic Distribution Technique to Minimize Packet Delivery Delay in Multi-Layered Satellite Networks. *IEEE Transactions on Vehicular Technology*, **62**, 3315-3324. http://dx.doi.org/10.1109/TVT.2013.2256812

[8] Lee, N., Kim, H., Chang, D. and Lee, H. (2007) Providing Seamless Services with Satellite and Terrestrial Network in Mobile Two Way Satellite Environments. *Managing Next Generation Networks and Services*, *Lecture Notes in Computer Science*, **4773**, 551-554. http://dx.doi.org/10.1007/978-3-540-75476-3_63

[9] Gopal, R. and Parthasarathy, V. (2014) MAW: Modified Algebraic Watchdog for Detecting and Mitigating the Misbehavior of Malicious Nodes in Cooperative Wireless Networks. *International Journal of Applied Engineering Research*, **9**, 22907-22920.

[10] Gopal, R. and Parthasarathy, V. (2015) HBSIDS: Improving Energy Efficiency of Human Body Sensor Based Intrusion Detection System in a Cooperative Network. *Australian Journal of Basic and Applied Sciences*, **9**, 551-558.

[11] Tomasin, S. (2011) Consensus-Based Detection of Malicious Nodes in Cooperative Wireless Networks. *IEEE Communications Letters*, **15**, 404-406. http://dx.doi.org/10.1109/LCOMM.2011.022411.102050

[12] Djenouri, D. and Badache, N. (2008) Struggling against Selfishness and Black Hole Attacks in MANETs. *Wireless Communications and Mobile Computing*, **8**, 689-704. http://dx.doi.org/10.1002/wcm.493

[13] Hussain, F.K., Chang, E. and Hussain, O.K. (2007) State of the Art Review of the Existing Bayesian-Network Based Approaches to Trust and Reputation Computation. *Second International Conference on Internet Monitoring and Protection*, 1-5 July 2007. http://dx.doi.org/10.1109/icimp.2007.43

[14] Buchegger, S. and Le Boudec, J.-Y. (2002) Performance Analysis of the Confidant Protocol: Cooperation of Nodes-Fairness in Distributed Ad Hoc Networks. *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing*, 9-11 June 2002, 226-236. http://dx.doi.org/10.1145/513800.513828

[15] Zhou, Y. and Ng, T.S. (2009) Performance Analysis on MIMO-OFCDM Systems with Mul-

ti-Code Transmission. *IEEE Transactions on Wireless Communications*, **8**, 4426-4433. http://dx.doi.org/10.1109/TWC.2009.081136

[16] Laneman, J.N., Tse, D.N.C. and Wornell, G.W. (2004) Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior. *IEEE Transactions on Information Theory*, **50**, 3062-3080. http://dx.doi.org/10.1109/TIT.2004.838089

[17] Gunduz, D. and Erkip, E. (2007) Opportunistic Cooperation by Dynamic Resource Allocation. *IEEE Transactions on Wireless Communications*, **6**, 1446-1454. http://dx.doi.org/10.1109/TWC.2007.348341

[18] Ikki, S. and Ahmed, M.H. (2007) Performance Analysis of Cooperative Diversity Wireless Networks over Nakagami-m Fading Channel. *IEEE Communications Letters*, **11**, 334-336. http://dx.doi.org/10.1109/LCOM.2007.348292

[19] Safari, M. and Uysal, M. (2008) Cooperative Diversity over Log-Normal Fading Channels: Performance Analysis and Optimization. *IEEE Transactions on Wireless Communications*, **7**, 1963-1972. http://dx.doi.org/10.1109/TWC.2008.070393

[20] Azgin, A., Altunbasak, Y. and AlRegib, G. (2005) Cooperative MAC and Routing Protocols for Wireless Ad Hoc Networks. *GLOBECOM'05 IEEE of Global Telecommunications Conference*, St. Louis, 28 November-2 December 2005, 2854-2859. http://dx.doi.org/10.1109/glocom.2005.1578280

[21] Korakis, T., Narayanan, S., Bagri, A. and Panwar, S. (2006) Implementing a Cooperative MAC Protocol for Wireless LANs. 2006 *IEEE International Conference on Communications*, San Francisco, 27 November-1 December 2006, 4805-4810. http://dx.doi.org/10.1109/icc.2006.255400

[22] Wyner, A.D. (1975) The Wire-Tap Channel. *Bell System Technical Journal*, **54**, 1355-1387. http://dx.doi.org/10.1002/j.1538-7305.1975.tb02040.x

[23] Leung-Yan-Cheong, S.K. and Hellman, M.E. (1978) The Gaussian Wiretap Channel. *IEEE Transactions on Information Theory*, **24**, 451-456. http://dx.doi.org/10.1109/TIT.1978.1055917

[24] Makda, S., Choudhary, A., Raman, N., Korakis, T., Tao, Z. and Panwar, S. (2008) Security Implications of Cooperative Communications in Wireless Networks. 2008 *IEEE in Sarnoff Symposium*, Princeton, 28-30 April 2008, 1-6. http://dx.doi.org/10.1109/SARNOF.2008.4520069

[25] Nadeem, A. and Howarth, M.P. (2014) An Intrusion Detection & Adaptive Response Mechanism for MANETs. *Ad Hoc Networks*, **13**, 368-380. http://dx.doi.org/10.1016/j.adhoc.2013.08.017

[26] Mitrokotsa, A. and Dimitrakakis, C. (2013) Intrusion Detection in MANET Using Classification Algorithms: The Effects of Cost and Model Selection. *Ad Hoc Networks*, **11**, 226-237. http://dx.doi.org/10.1016/j.adhoc.2012.05.006

[27] Thomas Paul Roy, A. and Balasubadra, K. (2015) DAD: A Secured Routing Protocol for Detecting and Preventing Denial-of-Service in Wireless Networks. *Wireless Personal Communications*, 1-15.

Scientific Research Publishing

Submit or recommend next manuscript to SCIRP and we will provide best service for you:

Accepting pre-submission inquiries through Email, Facebook, LinkedIn, Twitter, etc.
A wide selection of journals (inclusive of 9 subjects, more than 200 journals)
Providing 24-hour high-quality service
User-friendly online submission system
Fair and swift peer-review system
Efficient typesetting and proofreading procedure
Display of the result of downloads and visits, as well as the number of cited articles
Maximum dissemination of your research work

Submit your manuscript at: http://papersubmission.scirp.org/